Maiden Erlegh Trust

DATA PROTECTION POLICY

Initial approval:	May 2018
Review frequency:	Every three years
Date(s) reviewed:	May 2021

Contents

Statement of intent

Maiden Erlegh Trust is required to keep and process certain information about its staff members and pupils in accordance with its legal obligations under the Data Protection Act 1998 (DPA), and Data Protection Legislation 2018 (and revisions)

Data is processed for the educational benefit and wellbeing of all our students and staff. **Maiden Erlegh Trust** is working to maintain DPA compliance and all policies will be reviewed at an appropriate stage.

The Trust's schools may, from time to time, be required to share personal information about its staff or pupils with other organisations, mainly the LA, other schools and educational bodies, and potentially social services.

This policy is in place to ensure all staff and governors are aware of their responsibilities and outlines how the Trust complies with the following core principles of the DPA and has been approved by the directors of the Trust.

Organisational methods for keeping data secure are imperative, and **Maiden Erlegh Trust** believes that it is good practice to keep clear practical policies, backed up by written procedures.

Legal framework

This policy has due regard to legislation, including, but not limited to the following:

- Data Protection Act
- The Freedom of Information Act 2000
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016)
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- The School Standards and Framework Act 1998

This policy will also have regard to applicable guidance from the Information Commissioner's Office.

This policy will be implemented in conjunction with the appropriate other Trust policies.

Definition of Terms

For the purpose of this policy, **personal data/data subject** refers to information that relates to an identifiable, living individual, including information such as an online identifier, such as an IP address. The DPA legislation applies to both automated personal data and to manual filing systems, where personal data is accessible according to specific criteria, as well as to chronologically ordered data.

Sensitive personal data is referred to in the DPA as 'special categories of personal data', which are broadly the same as those in the Data Protection Act (DPA) 1998. These specifically include the processing of genetic data, biometric data and data concerning health matters.

A **personal data breach** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes.

Principles

In accordance with the requirements outlined in the DPA, personal data will be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals.
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- Accurate and, where necessary, kept up-to-date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods, insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the DPA in order to safeguard the rights and freedoms of individuals.

- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

The DPA also requires that "the controller shall be responsible for, and able to demonstrate, compliance with the principles".

Accountability

Maiden Erlegh Trust will implement appropriate technical and organisational measures to demonstrate that data is processed in line with the principles set out in the DPA.

The trust will provide comprehensive, clear and transparent privacy policies.

Additional internal records of the trust's processing activities will be maintained and kept up-to-date.

Internal records of processing activities will include the following:

- Name and details of the organisation

- Purpose(s) of the processing

- Description of the categories of individuals and personal data

- Retention schedules

- Categories of recipients of personal data

- Description of technical and organisational security measures

- Details of transfers to third countries, including documentation of the transfer mechanism safeguards in place

The trust will implement measures that meet the principles of data protection by design and data protection by default, such as:

- Data minimisation.

- Transparency.

- Allowing individuals to monitor processing.

- Continuously creating and improving security features.

Data protection impact assessments will be used, where appropriate.

Data protection officer (DPO)

A DPO is appointed in order to:

- Inform and advise the Trust and its employees about their obligations to comply with the DPA and other data protection laws.

- Monitor the Trust's schools compliance with the DPA and other laws, including managing internal data protection activities, advising on data protection impact assessments, conducting internal audits, and providing the required training to staff members.

- An existing employee will be appointed to the role of DPO provided that their duties are compatible with the duties of the DPO and do not lead to a conflict of interests.

The DPO will report to the highest level of management at the Trust, which is the nominated Trust governor.

The DPO will operate independently and will not be dismissed or penalised for performing their task.

Sufficient resources will be provided to the DPO to enable them to meet their DPA obligations.

Lawful processing

The legal basis for processing data will be identified and documented prior to data being processed.

For Personal Data to be processed lawfully, certain conditions have to be met. These may include:

- The consent of the data subject has been obtained.

- Processing is necessary for:
  - Compliance with a legal obligation.

  - The performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

  - For the performance of a contract with the data subject or to take steps to enter into a contract.

  - Protecting the vital interests of a data subject or another person.

  - For the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject.

Sensitive personal data will only be processed under the following conditions:

- Explicit consent of the data subject, unless reliance on consent is prohibited UK law.

- Processing carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without consent.

- Processing relates to personal data manifestly made public by the data subject.

- Processing is necessary for:
  - Carrying out obligations under educational, employment, social security or social protection law, or a collective agreement.

  - Protecting the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent.

  - The establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity.

  - Reasons of substantial public interest on the basis UK law which is proportionate to the aim pursued and which contains appropriate safeguards.

  - The purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis UK law or a contract with a health professional.

  - Reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices.

  - Archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 89(1).

Consent

Consent must be a positive indication. It cannot be inferred from silence, inactivity or pre-ticked boxes.

Consent will only be accepted where it is freely given, specific, informed and an unambiguous indication of the individual's wishes.

Where consent is given, a record will be kept documenting how and when consent was given.

The Trust's schools ensure that consent mechanisms meet the standards of the DPA. Where the standard of consent cannot be met, an alternative legal basis for processing the data must be found, or the processing must cease.

Consent accepted under the DPA will be reviewed to ensure it meets the standards of the DPA; however, acceptable consent obtained under the DPA will not be reobtained.

Consent can be withdrawn by the individual at any time.

The consent of parents will be sought prior to the processing of a child's data, except where the processing is related to preventative or counselling services offered directly to a child.

The right to be informed

The privacy notice supplied to individuals in regards to the processing of their personal data will be written in clear, plain language which is concise, transparent, easily accessible and free of charge.

If services are offered directly to a child, the Trust will ensure that the privacy notice is written in a clear, plain manner that the child will understand.

In relation to data obtained both directly from the data subject and not obtained directly from the data subject, the following information will be supplied within the privacy notice:

- The identity and contact details of the controller, and where applicable, the controller's representative and the DPO.
- The purpose of, and the legal basis for, processing the data.
- The legitimate interests of the controller or third party.
- Any recipient or categories of recipients of the personal data.
- Details of transfers to third countries and the safeguards in place.
- The retention period of criteria used to determine the retention period.
- The existence of the data subject's rights, including the right to:
    - Withdraw consent at any time.
    - Lodge a complaint with a supervisory authority.

Where data is obtained directly from the data subject, information regarding whether the provision of personal data is part of a statutory or contractual requirement and the details of the categories of personal data, as well as any possible consequences of failing to provide the personal data, will be provided.

Where data is not obtained directly from the data subject, information regarding the source the personal data originates from and whether it came from publicly accessible sources, will be provided.

For data obtained directly from the data subject, this information will be supplied at the time the data is obtained.

In relation to data that is not obtained directly from the data subject, this information will be supplied:

- Within one month of having obtained the data.
- If disclosure to another recipient is envisaged, at the latest, before the data are disclosed.
- If the data are used to communicate with the individual, at the latest, when the first communication takes place.

The right of access

Individuals have the right to obtain confirmation that their data is being processed.

Individuals have the right to submit a subject access request (SAR) to gain access to their personal data in order to verify the lawfulness of the processing.

The trust will verify the identity of the person making the request before any information is supplied. (More details are in the Subject Access Request procedure)

A copy of the information will be supplied to the individual free of charge; however, the Trust's schools may impose a 'reasonable fee' to comply with requests for further copies of the same information.

Where a SAR has been made electronically, the information will be provided in a commonly used electronic format. The trust reserves the right to verify the identity of the person making the SAR by an alternative means.

Where a request is manifestly unfounded, excessive or repetitive, a reasonable fee will be charged.

All fees will be based on the administrative cost of providing the information.

All requests will be responded to without delay and at the latest, within one month of receipt. There may be exceptions to this time scale – see the SAR procedure.

In the event of numerous or complex requests, the period of compliance will be extended by a further two months. The individual will be informed of this extension, and will receive an explanation of why the extension is necessary, within one month of the receipt of the request.

Where a request is manifestly unfounded or excessive, the trust holds the right to refuse to respond to the request. The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the supervisory authority and to a judicial remedy, within one month of the refusal.

In any event, the trust will ask the individual to specify the information the request is in relation to.

The right to rectification

Individuals are entitled to have any inaccurate or incomplete personal data rectified.

Where the personal data in question has been disclosed to third parties, the Trust's schools will inform them of the rectification where possible.

Where appropriate, the Trust's schools will inform the individual about the third parties that the data has been disclosed to.

Requests for rectification will be responded to within one month; this will be extended by two months where the request for rectification is complex.

Where no action is being taken in response to a request for rectification, the trust will explain the reason for this to the individual, and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

The right to erasure

Individuals hold the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

Individuals have the right to erasure in the following circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed
- When the individual withdraws their consent
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing
- The personal data was unlawfully processed
- The personal data is required to be erased in order to comply with a legal obligation
- The personal data is processed in relation to the offer of information society services to a child

The trust has the right to refuse a request for erasure where the personal data is being processed for the following reasons:

- To exercise the right of freedom of expression and information
- To comply with a legal obligation for the performance of a public interest task or exercise of official authority
- For public health purposes in the public interest
- For archiving purposes in the public interest, scientific research, historical research or statistical purposes
- The exercise or defence of legal claims

As a child may not fully understand the risks involved in the processing of data when consent is obtained, special attention will be given to existing situations where a child has given consent to processing and they later request erasure of the data, regardless of age at the time of the request.

Where personal data has been disclosed to third parties, they will be informed about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so.

Where personal data has been made public within an online environment, the Trust will inform other organisations who process the personal data to erase links to and copies of the personal data in question.

The right to restrict processing

Individuals have the right to block or suppress the trust's processing of personal data where that processing falls outside the legal obligation for the performance of a public interest task or exercise of official authority

In the event that processing is restricted, the trust will store the personal data, but not further process it, guaranteeing that just enough information about the individual has been retained to ensure that the restriction is respected in future.

The trust will restrict the processing of personal data in the following circumstances:

- Where an individual contests the accuracy of the personal data, processing will be restricted until the Trust's school has verified the accuracy of the data
- Where an individual has objected to the processing and the trust is considering whether their legitimate grounds override those of the individual
- Where processing is unlawful and the individual opposes erasure and requests restriction instead
- Where the trust no longer needs the personal data but the individual requires the data to establish, exercise or defend a legal claim

If the personal data in question has been disclosed to third parties, the trust will inform them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so.

The trust will inform individuals when a restriction on processing has been lifted.

The right to data portability

Individuals have the right to obtain and reuse their personal data for their own purposes across different services.

Personal data can be easily moved, copied or transferred from one IT environment to another in a safe and secure manner, without hindrance to usability.

The right to data portability only applies in the following cases:

- To personal data that an individual has provided to a controller
- Where the processing is based on the individual's consent or for the performance of a contract
- When processing is carried out by automated means

Personal data will be provided in a structured, commonly used and machine-readable form.

The trust will provide the information free of charge.

Where feasible, data will be transmitted directly to another organisation at the request of the individual.

Maiden Erlegh Trust is not required to adopt or maintain processing systems which are technically compatible with other organisations.

In the event that the personal data concerns more than one individual, the trust will consider whether providing the information would prejudice the rights of any other individual.

The trust will respond to any requests for portability within one month.

Where the request is complex, or a number of requests have been received, the timeframe can be extended by two months, ensuring that the individual is informed of the extension and the reasoning behind it within one month of the receipt of the request.

Where no action is being taken in response to a request, the trust will, without delay and at the latest within one month, explain to the individual the reason for this and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

The right to object

The trust will inform individuals of their right to object at the first point of communication, and this information will be outlined in the privacy notice and explicitly brought to the attention of the data subject, ensuring that it is presented clearly and separately from any other information.

Individuals have the right to object to the following:

- Processing based on legitimate interests or the performance of a task in the public interest
- Direct marketing
- Processing for purposes of scientific or historical research and statistics.

Where personal data is processed for the performance of a legal task or legitimate interests:

- An individual's grounds for objecting must relate to his or her particular situation.
- The trust will stop processing the individual's personal data unless the processing is for the establishment, exercise or defence of legal claims, or, where the trust can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual.

Where personal data is processed for direct marketing purposes:

- The trust will stop processing personal data for direct marketing purposes as soon as an objection is received.
- The trust cannot refuse an individual's objection regarding data that is being processed for direct marketing purposes.

Where personal data is processed for research purposes:

- The individual must have grounds relating to their particular situation in order to exercise their right to object.
- Where the processing of personal data is necessary for the performance of a public interest task, the Trust is not required to comply with an objection to the processing of the data.

Where the processing activity is outlined above, but is carried out online, the trust will offer a method for individuals to object online.

Privacy by design and privacy impact assessments

The trust will act in accordance with the DPA by adopting a privacy by design approach and implementing technical and organisational measures which demonstrate how the trust has considered and integrated data protection into processing activities.

Data protection impact assessments (DPIAs) will be used to identify the most effective method of complying with the Trust's data protection obligations and meeting individuals' expectations of privacy.

DPIAs will allow the Trust to identify and resolve problems at an early stage, thus reducing associated costs and preventing damage from being caused to **Maiden Erlegh Trust's** reputation which might otherwise occur.

A DPIA will be used when using new technologies or when the processing is likely to result in a high risk to the rights and freedoms of individuals.

A DPIA will be used for more than one project, where necessary.

High risk processing includes, but is not limited to, the following:

- Systematic and extensive processing activities, such as profiling
- Large scale processing of special categories of data or personal data which is in relation to criminal convictions or offences

The Trust will ensure that all DPIAs include the following information:

- A description of the processing operations and the purposes
- An assessment of the necessity and proportionality of the processing in relation to the purpose
- An outline of the risks to individuals
- The measures implemented in order to address risk

Where a DPIA indicates high risk data processing, the trust will consult the ICO to seek its opinion as to whether the processing operation complies with the DPA.

Data breaches

The term 'personal data breach' refers to a breach of security which has led to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

The DPO will ensure that all staff members are made aware of, and understand, what constitutes as a data breach as part of their continuous development training.

Where a breach is likely to result in a risk to the rights and freedoms of individuals, the relevant supervisory authority will be informed.

All notifiable breaches will be reported to the relevant supervisory authority within 72 hours of the Trust becoming aware of it.

The risk of the breach having a detrimental effect on the individual, and the need to notify the relevant supervisory authority, will be assessed on a case-by-case basis.

In the event that a breach is likely to result in a high risk to the rights and freedoms of an individual, the Trust will notify those concerned directly.

A 'high risk' breach means that the threshold for notifying the individual is higher than that for notifying the relevant supervisory authority.

In the event that a breach is sufficiently serious, the public will be notified without undue delay.

Effective and robust breach detection, investigation and internal reporting procedures are in place at the Trust's schools, which facilitate decision-making in relation to whether the relevant supervisory authority or the public need to be notified.

Within a breach notification, the following information will be outlined:

- The nature of the personal data breach, including the categories and approximate number of individuals and records concerned
- The name and contact details of the DPO
- An explanation of the likely consequences of the personal data breach
- A description of the proposed measures to be taken to deal with the personal data breach
- Where appropriate, a description of the measures taken to mitigate any possible adverse effects

Failure to report a breach when required to do so will result in disciplinary procedures.

Data security

Confidential paper records will be kept in a locked filing cabinet, drawer or safe, with restricted access.

Confidential paper records will not be left unattended or in clear view anywhere with general access.

Digital data is coded, encrypted or password-protected, both on a local hard drive and on a network drive that is regularly backed up off-site.

Where data is saved on removable storage or a portable device, the device will be kept in a locked filing cabinet, drawer or safe when not in use.

Memory sticks will not be used to hold personal information unless they are password-protected and fully encrypted.

All electronic devices are password-protected to protect the information on the device in case of theft.

Where possible, the trust enables electronic devices to allow the remote blocking or deletion of data in case of theft.

All necessary members of staff are provided with their own secure login and password, and every computer regularly prompts users to change their password.

Emails containing sensitive or confidential information are password-protected if there are unsecure servers between the sender and the recipient.

Circular emails to parents are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients.

When sending confidential information by fax, staff will always check that the recipient is correct before sending.

Where personal information that could be considered private or confidential is taken off the premises, either in electronic or paper format, staff will take extra care to follow the same procedures for security, e.g. keeping devices under lock and key. The person taking the information from the Trust's premises accepts full responsibility for the security of the data.

Before sharing data, all staff members will ensure:

- They are allowed to share it.
- That adequate security is in place to protect it.
- Who will receive the data has been outlined in a privacy notice.

Under no circumstances are visitors allowed access to confidential or personal information. Visitors to areas of the Trust's schools containing sensitive information are supervised at all times.
The physical security of the Trust's school buildings and storage systems, and access to them, is reviewed on a **regular** basis. If an increased risk in vandalism/burglary/theft is identified, extra measures to secure data storage will be put in place.

Maiden Erlegh Trust takes its duties under the DPA seriously and any unauthorised disclosure may result in disciplinary action.

The **Chief Financial and Operations Officer (CFOO)** is responsible for continuity and recovery measures are in place to ensure the security of protected data.

Publication of information

Maiden Erlegh Trust publishes a publication scheme on its website outlining classes of information that will be made routinely available, including:

- Policies and procedures
- Minutes of meetings
- Annual reports
- Financial information

Classes of information specified in the publication scheme are made available quickly and easily on request.

Maiden Erlegh Trust will not publish any personal information, including photos, on its website without the permission of the affected individual.

When uploading information to the Trust's school websites, staff are considerate of any metadata or deletions which could be accessed in documents and images on the site.

CCTV and photography

The trust understands that recording images of identifiable individuals constitutes as processing personal information, so it is done in line with data protection principles.

The trust notifies all pupils, staff and visitors of the purpose for collecting CCTV images via notice boards, letters and email.

Cameras are only placed where they do not intrude on anyone's privacy and are necessary to fulfil their purpose.

All CCTV footage will be kept for at least six months for security purposes; the CFOO is responsible for keeping the records secure and allowing access.

The trust will always indicate its intentions for taking photographs of pupils and will retrieve permission before publishing them.

If the trust wishes to use images/video footage of pupils in a publication, such as the Trust's websites, prospectus, or recordings of Trust's school plays, written permission will be sought for the particular usage from the parent of the pupil.

Images captured by individuals for recreational/personal purposes, and videos made by parents for family use, are exempt from the DPA.

Biometric data

Currently Biometric Data is not in use in any of the educational establishments across the Trust, however should this situation change this policy will be amended as appropriate. Any data subjects will be informed of any such change and this Biometric data will be handled in line with any legislation live at the time and also in line with any appropriate guidance issued by the DfE

Data retention

Data will not be kept for longer than is necessary in line with the Trust's data retention protocol.

Unrequired data will be deleted as soon as practicable.

Some educational records relating to former pupils or employees of the Trust may be kept for an extended period for legal reasons, but also to enable the provision of references or academic transcripts.

Paper documents will be shredded or pulped, and electronic memories scrubbed clean or destroyed, once the data should no longer be retained.

Authorised Disclosures/DBS data

All data provided by the DBS or any Authorised Disclosures will be handled in line with data protection legislation; this includes electronic communication.

Data provided by the DBS will never be duplicated.

Any third parties who access DBS information will be made aware of the data protection legislation, as well as their responsibilities as a data handler.

Policy review

This policy is reviewed every **three years** by the **DPO** and the **Chief Financial and Operations Officer**

The next scheduled review date for this policy is **May 2021**

There will be a number of procedures linked to this policy which will be added and the appropriate appendices.

Appendix 1: MET Cyber Security Management 2021

Cyber security principles & processes

The below principals and processes are complementing the MET Data Protection Policy.

Data and Infrastructure Security

1. Access to systems, which stores business and personal data is designed and granted to authenticated and authorised staff only. Staff user accounts are protected with password and MFA (multi-factor authentication) which enforces extra security if user authenticate from outside of secure locations (schools' networks).
    a. Staff can opt out of MFA, but they will not be allowed access to Remote Desktop Services and Microsoft 365 from outside the school. More systems currently accessible via the Internet without MFA are expected to be added in the future as their technology allows integration with MFA.

2. All MET workstations and servers have installed **managed** antivirus software.

3. MET apps where possible use secure connections to databases and data feeds.

4. Servers hosted in Public cloud data centres, use encrypted storage.

5. Connection between the offices use encrypted IPSec or Branch Office Virtual Private Network technology/tunnels.

6. Remote Access Servers are only accessible from outside by users behind MFA.

7. All email traffic via the Office 365 platform is protected by malware and it is routed via RM's FortiGate Antispam platform for the **maidenereghtrust.org** domain and via the O365 own antispam platform for every other domain.
    a. The "**maidenerleghschools.co.uk**" used by Google Classroom environment is using Google's own secure email gateway.
    b. An additional safeguard for phishing emails that attempt to impersonate MET staff, has been set up to deny delivery of such emails and divert them to the ICT Manager for approval or rejection. Albeit this process can delay the delivery of genuine emails to the final recipient, it is necessary to protect MET from phishing related email attacks.

8. Schools that that use RM Broadband are also using RMs SafeNet web proxy. Schools that are not on RM Broadband have UTM (Unified Threat Management) class firewall, which has security functions enabled, including Web Proxy.

Access to systems and passwords

Access to all the MET IT systems is controlled using User IDs, passwords and tokens. All User IDs and passwords are to be uniquely assigned to named individuals and consequently, individuals are accountable for all actions on the MET IT systems.

The MET Password - Operating Procedure, available on the intranet is enforced at all times, including the statement "**We never share our passwords with anyone**".

System owners, which may not necessarily be the IT Team, are required to change any vendor-supplied defaults for system passwords and other security parameters. This includes all hardware and software systems that are supplied with default administrative or operational accounts.

The copying, transferring and storing of data onto local hard drives and removable media, unless explicitly authorized for a defined school requirement is not allowed. Local hard drives also include the user's workstation desktop environment and the user's remote desktop. Laptop users may not copy MET's sensitive data to their laptop's desktop.

Antivirus software

There is a constant stream of attacks using widely published exploits against computer systems. Without Antivirus (AV) software that is updated regularly, these forms of malicious software can attack and disable any network including MET's.

Malicious software may be unknowingly downloaded or installed from the Internet (directly or via a web link on an email), but computers are also vulnerable when using removable storage devices such as USB memory sticks and hard drives, smartphones, and other peripheral devices. Without AV software installed, these computers may become access points into MET's network, or maliciously target information within the network.

AV software must be therefore deployed on all systems commonly affected by malicious software. This should include all MET workstations, regardless of if it is a desktop or a laptop and all Windows servers.

An AV platform should be capable of both file protection and scanning network traffic against malicious software like: (viruses, Trojans, worms, spyware, adware, and rootkits etc.).

The AV platform must be centrally managed and include a reporting management console where all security events and audit logs from stations are recorded, as even the best AV software is limited in effectiveness if it does not have current anti-virus signatures or if it is not active on a server on an individual's computer.

It is paramount that the AV virus definitions are updated frequently. In addition, the master installation of the software must be set to receive automatic updates from the platform's developer. Finally, the AV software must be set to perform periodic scans.

Audit logs should provide the ability to monitor virus activity and AV reactions. It is imperative that the AV software is configured to generate audit logs and that those logs are managed appropriately. One way to have visibility of AV activity is via email notification to IT of certain AV activity e.g., potential infection on a station. MET's IT Team has configured the current AV Management console to explore and utilise the AV platform notification system to that extent.

As industry trends for malicious software can change quickly, the IT department at MET is responsible for identifying and addressing new security vulnerabilities and update the configuration standards and processes accordingly.

Patch Management

1. Operating systems, databases, and enterprise applications should be updated frequently with security patches to allow fixes of known security vulnerabilities.

2. All Windows workstations are patched on a daily basis, and this process is automatic.

3. All Virtual servers are patched once a month with the latest security updates. The physical servers are patched once every two months with the latest security updates. Such updates tend to be carried out off hours, with communication messages sent to users about expected downtime as applicable.

4. Other devices such as Chromebook, iPads etc, are updated on a more ad-hoc basis, but typically once a year.

5. Backend devices such as Firewall, Switches, Storage Servers & Wi-Fi Access Points are checked for firmware updates on a more ad-hoc basis, but typically once a year. Some updates are ignored (intentionally) and some need to be applied ASAP due to a known vulnerability. Such updates tend to be carried out off hours, with communication messages sent to users about expected downtime as applicable.

6. Software applications, other than the Operating System, depending on their nature are checked for latest releases on a more ad-hoc basis, but typically once a year.

Backups

The MET has backup systems in place to backup all systems and data. The backup systems will include all files stored on the school's network, MIS databases such as SIMS, where teacher assessed grades are stored, as well as Microsoft 365 data such as email and SharePoint stored on the cloud.

MET is utilising hard disk-based backup technology, as oppose to tape, and uses a product called Redstor, which backups up all **internal servers for all schools** and sends them to a Cloud based storage facility of Redstor once a day. Backups are retained for a period of 6 months.

Utilising the Redstor platform, MET IT can recover files, folders, whole volumes/disks or whole servers. Recovery times vary depending on amount of restored data. Typically, data restoration works out at about 40GB per hour.

Those backups are held offline, and there is no live and direct access to the backed data from the internal server environment, thus guarantee a physical separation from the live/production environment. To load the backups for restoration purposes, the Redstor Platform will need to be explicitly used by the IT Team, use dedicated credentials to log on to it, and mount the data and process the restore.

Testing of Redstor to ensure data can be restored, is a frequent exercise due to requests by users to recover deleted files from the internal File services. Loading of MIS databases from a past backup and recovery of a random server as a whole is annual exercise.

For Microsoft 365 data, MET makes use of a "**Global Retention Policy for Office 365**" data, which makes use of the "**Preservation Hold Library**" system for SharePoint stored data.

Disaster Recovery

Power
MET has all the servers and major networking equipment connected to UPS devices. This will protect equipment for sudden electrical surges and in the event of a power outage, they will power the equipment for about 30 minutes.

Server failures

MET is utilising the benefit of a Storage Area Network (SAN) as well as Server Clustering technology. In the event of a failure of a physical server, a different physical server will be taking over, and this process has been automated. It is likely that some servers will have their optimal performance deteriorated in such scenario, and IT may not run some less critical server/services until the physical server is repaired.

Disks/SAN Storage failures
MET is utilising RAID technology and highly redundant storage systems, and if up to 2-4 (depending on the storage system) disks fail simultaneously, there will be no loss of system access. It is possible that some servers will have their optimal performance deteriorated, however.

Hardware replacement scheme
There is a hardware warranty scheme for all critical network items in place. E.g., Servers, and storage systems. Hardware replacement timeframes ranges from between 4 hours and next business day depending on equipment.

Data Lines
Only Maiden Erlegh School has a second line, and if the main data line goes down an alternative backup line will take over. This process has been configured to work automatically (auto fail over), with very minimal (if any) downtime. As this is a backup line, bandwidth is inferior to the main fibre optic quality line, and some less critical services may be stopped from running, in order to conserve bandwidth, until the main line is restored.

Spare equipment and auto-fail over for critical networking devices
Depending on the school, and system, there are some spare/redundant systems such as the Wi-Fi Controller or spare switches for some schools, but some other networking equipment such as Firewalls & Routers have not currently been designed with auto-fail over capability/High Availability and will rely on vendor support contract to replace it or repair it.

Microsoft 365 Services/Google Services
There are currently no alternative access mediums to email or SharePoint data or google cloud data in the event of either Microsoft 365 Services or Google Services becomes unavailable. We will rely on those provides to restore their services.

About Ransomware incidents

It is vital at MET that we have a number of your existing defences and take the necessary steps to protect our networks from cyber-attacks, including Ransomware.
In the unlikely event of infections from ransomware, the DfE supports the National Crime Agency's recommendations not to encourage, endorse, or condone the payment of ransom demands. Payment of ransoms has no guarantee of restoring access or services and will likely result in repeat incidents to educational settings.

Along with our defences, having the ability to restore the systems and recover data from backups is vital. To that effect; the MET has backup systems in place to backup all systems and data.

IT Infrastructure Security (for the IT Team)

Configuration standards (general)

1. MET's ICT Manager should develop certain configuration standards for all system components.

    a. Default services and protocols that are not needed or utilised by MET's IT environment must be switched off or disabled.

    b. Default access accounts need to be disabled or changed to non-default.

    c. When applicable, a service or protocol should be narrowed in scope to allow MET's specific only access e.g., the SNMP protocol of each site router is enabled but narrowed in scope to allow only certain IP address to probe it.

    d. System configurations standards need to be updated as new vulnerability issues are identified.

    e. Operating systems, databases, and enterprise applications should be updated frequently with security patches to allow fixes of known security vulnerabilities – according to "Patch Management Policy".

    f. System configurations standards need to be defined for all new systems implemented.

    g. All enabled insecure services, daemons, or protocols should be justified and such configuration standards, should be documented.

2. System configuration standards should also be kept up to date to ensure that newly identified weaknesses are corrected prior to a system being installed on the network.

3. System configuration standards should be applicable when new systems are procured, set up and configured e.g. a new server is introduced.

4. As a general rule, only one primary function should be implemented per server, to prevent functions that require different security levels from co-existing on the same server. The ICT Manager should justify any deviation from this standard.

5. Only necessary services, protocols etc. should be enabled as required for servers and systems. Any services and protocols not directly needed to perform the device's specific function should be disabled e.g. use of Telnet and other insecure remote login commands should be disabled when not required.

6. All enabled insecure services, daemons, or protocols should be justified by the ICT Manager.

7. Inter-site traffic via IPSec or BO VPN should be set up to protect information flow between the two MET's sites.

8. All critical non-console administrative access should be encrypted with strong and safe cryptography. e.g. access via the web interface for Proxy, Antivirus, firewall should be accessible via https

Security Incident Response Plan

What is an incident
A Security Incident means any incident that occurs by accident or deliberately that impacts MET's communications or IT systems. An incident may be any event or set of circumstances that threatens the confidentiality, integrity or availability of information, data or services in MET.

This includes unauthorised access to, use, disclosure, modification, or destruction of data or services used or provided by MET.

How to Recognise a Security Incident
A security incident may not be recognised straightaway; however, there may be indicators of a security breach, system compromise, unauthorised activity, or signs of misuse within MET environment.

MET IT Team needs to look out for any indications that a security incident has occurred or may be in progress, some of which are outlined below:

1. Monitor excessive or unusual log-in and system activity, in particular from any inactive user IDs (user accounts).

2. Watch out for excessive or unusual remote access activity.

3. The occurrence of spoofing new wireless (Wi-Fi) networks visible or accessible from our environment.

4. The presence of or unusual activity in relation to malware (malicious software), suspicious files, or new/unapproved executables and programs.

5. Hardware or software key-loggers found connected to or installed on systems.

6. Suspicious or unusual activity on, or behaviour of, Web-facing systems.

7. Lost, stolen, or misplaced computers, laptops, hard drives, or other media devices that contain sensitive data

Roles and Responsibilities

Incident response plan must be followed by all personnel at MET. This includes not just permanent MET staff, but temporary staff, consultants, contractors, suppliers and third parties operating on behalf of MET working with MET's customers' data or on MET premises. For simplicity, all of these personnel are referred to as 'staff' within this plan.

The MET Security Incident Response Team (SIRT) is formed of:

Role	**SIRT Responsibility**
ICT Manager	Incident Response Lead
CEO	Executive Officer/Risk Owner
DPO	Handling of GDPR procedures
CFOO	Handling of any personnel and disciplinary issues relating to security incidents and communication of Cyber Security Policy.
CFOO	Handling of any external communications in relation to an incident (like customers' data leak)

The Incident Response Lead is responsible for:

1. Leading the investigation of a suspected breach or reported security incident and initiating the Security Incident Response Plan, as and when needed.

2. Reporting to and liaising with external parties, law enforcement, etc. as is required.

3. Making sure that the Security Incident Response Plan and associated response and escalation procedures are defined and documented. This is to make sure that the handling of security incidents is timely and effective.

4. Making sure that the Security Incident Response Plan is up-to-date and reviewed frequently.

5. Making sure that staff with Security Incident Response Plan responsibilities are properly trained.

6. Investigating each reported incident.

7. Gathering, reviewing and analysing logs and related information from various central and local safeguards, security measures and controls.

8. Documenting and maintaining accurate and detailed records of the incident and all activities that were undertaken in response to an incident with use of helpdesk system.

9. Resolving each incident to the satisfaction of all parties involved, including external parties.

10. Initiating follow-up actions to reduce likelihood of recurrence, as appropriate.

11. Determining if policies, processes, technologies, security measures or controls need to be updated to avoid a similar incident in the future. They also need to consider whether additional safeguards are required in the environment where the incident occurred.

12. Make sure that all staff understand how to identify and report a suspected or actual security incident.

Scenario planning and scenario evaluation

The ICT Manager is responsible for drafting relevant scenarios linked to Cyber Security and disaster related events and evaluate them.